Technical Guideline BSI TR-03119

Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control

Version 1.3

22. March 2013

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn, Germany

Email: ePA@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Introduction 5
2 Interoperable Smart Card Reader 5
2.1 Terminal Definition 6
2.2 Architecture 6
2.3 Certification 6
3 Categories of Smart Card Readers 7
3.1 Basic Reader (Cat-B) 7
3.2 Standard Reader (Cat-S) 8
3.3 Comfort Reader (Cat-K) 8
4 General Recommendations 8
4.1 Utilisation Processes and Use Cases 9
4.2 Fundamental Requirements and Assumptions 9
4.3 Interfaces 10
A Modules 12
A.1 Interface to the Host Computer 12
A.2 Contactless Interface 13
A.3 Contact Interface 14
A.4 PIN Pad Supporting PACE 15
A.5 Display 16
A.6 QES with Contact Cards 19
A.7 QES with Contactless Cards according to TR-03117 19
A.8 Firmware Update 21
B Certification Requirements 21
B.1 Interface to the Host Computer 21
B.2 Contactless Interface 21
B.3 Contact Interface 22
B.4 PIN Pad with PACE Support 22
B.5 Display 22
B.6 QES with Contact Cards 22
B.7 QES with Contactless Cards according to TR-03117 23
B.8 Firmware Update 23
C Functional Tests 23
C.1 General Requirements 23
C.2 Tests 24
C.3 Test Report 28
D Support for PACE and EAC 29
D.1 Commands 29
D.2 Mapping on PC/SC 32
D.3 Mapping on CCID 33
E IT Security Evaluation 34

Index of Tables

Table 1: Overview of Smart Card Reader Categories....7
Table 2: Command Overview GetReaderInfo....13
Table 3: Standard Display Texts....17

Version	*Date*	*Changes*
1.1	15.12.09	Version 1.1 of the Technical Guideline
1.2	27.05.11	Basic revision, error corrections, practical experiences taken into account
1.3	22.03.13	English translation, CCID host interface

1 Introduction

The German electronic ID card combines the conventional identity card with three new electronic functions in the credit card format:

- Mutual electronic proof of identity (eID function) for eBusiness and eGovernment applications
- Qualified Electronic Signature (eSign function) according to the German Electronic Signature Act for eBusiness and eGovernment applications
- Electronic identification for exclusive governmental use.

The data is stored on an RF chip integrated in the smart card. The communication between the chip and a contactless smart card reader is carried out via an inductive coupling compliant to [ISO 14443].

To protect information and ensure its confidentiality, integrity and availability, only secure IT products must be employed. This imposes high requirements in functionality and security on smart card readers.

This technical guideline serves as a foundation for mutually compatible smart card readers which can also be used for other applications. It enables application developers to establish a uniform interface for deploying smart card readers by arbitrary manufacturers which are compliant to this Technical Guideline.

The most important requirement for a smart card reader is a faultless, interference-free and reliable operation as well as the integrity of the smart cards. This is why detailed requirements and further functions have to be specified to ensure the interoperability of both contact and contactless smart card readers. Finally, information security must be taken into account as well to ensure the confidentiality and the integrity of the processes and the communication.

Compatible approaches from national and international standards, policies and guidelines have been taken into consideration.

Scope of the Technical Guideline

This technical guideline for contact and contactless smart card readers is intended primarily for equipment to be used with the identity card and in further smart card projects of the Federal Administration, where non-governmental applications can be involved. Since a card reader for personal identification by the Executive must have different characteristics from a smart card reader for an authentication or an electronic signature, these card readers are not in the scope of this Technical Guideline.

This document describes individual modules for individual use cases as based on the special requirements pertaining to the use case. Combining mandatory and optional modules will result in a specification of practical variants of smart card readers, which are defined in this Technical Guideline and supplemented by certification requirements.

2 Interoperable Smart Card Reader

This guideline defines card readers for the use with the eID and QES functions of the new German electronic identity card.

It is sometimes also required to use the same smart card reader for smart cards supporting other applications (health card, signature card, money card). Therefore in the following sections variants of smart card readers are described which allow for multifunctional use with other applications.

All smart card readers described here are to be used primarily with the identity card and the contactless smart card interface. The contact smart card interface has also been taken into account. After the presentation of basic characteristics and requirements, Chapter 3 provides a detailed specification for selected categories of smart card readers.

2.1 Terminal Definition

Smart card reader devices can have different characteristics due to different usages and different applications. The variety ranges from simple smart card interfaces without a keyboard and display to sophisticated smart card reader devices with proprietary applications for extended security-relevant functions. These smart card readers are often also called card terminals.

The transition from a smart card reader, which is essentially responsible for the communication between the smart card and the host, and a card terminal with extended functions is fluid.

This guideline does not explicitly distinguish between a smart card reader and a card terminal. The term smart card reader will be used independently of the actual characteristics.

2.2 Architecture

Due to the variety of smart card readers and the originally required interoperable objectives as well as to provide a foundation for a product qualification, a classification of the specific characteristics of a smart card reader in terms of individual modules will be defined. The smart card, the reader and their functional components (a keyboard, a display, etc.) are controlled by commands specified in[CCID]/[PC/SC] and APDUs according to [ISO 7816] as well as other optional APIs.

In contrast to smart card readers for personal use, where it is important that the application programming is flexible and can be easily developed, other special requirements come into play when system readers are in focus. System readers are not subject of this Technical Guideline.

If a module is not required by specific reader characteristics, the modules can be used **optionally**. If a functionality is used in a smart card reader and this function of the reader's characteristics is described as a module, this module has to be implemented for interoperability reasons. In Chapter 3 the specific characteristics are described, resulting from the requirements of the individual applications (use cases).

Chapter 4 contains general recommendations, Appendix A provides a detailed description of the modules.

2.3 Certification

Smart card reader manufacturers can apply for a conformity evaluation according to the Technical Guideline BSI TR-03119 for their products and obtain a certificate confirming such adherence.

For granting of a certificate by the BSI, a successful conformity evaluation in accordance with the requirements defined in this guideline (Appendix B) is a prerequisite. Conformity evaluations are carried out by independent (commercial) evaluation facilities, recognized by the BSI according to DIN ISO/IEC 17025. Responsibility for choosing and commissioning one or more suitable evaluation facilities lies with the applicant.[1]

A protocol of all tests performed during the conformity evaluation and a final test report summarising the results are provided by the respective evaluation facility.

1 A list of all evaluation facilities authorised to perform conformity evaluations according to Technical Guidelines is published on the BSI website.

The certification authority at the BSI supervises the conformity evaluation and grants the certificate applied for after a successful conclusion of the evaluation and on the basis of all test reports.

Granted certificates are published by the BSI.

In addition, certified smart card readers are labelled with the BSI test seal indicating a successful certification according to BSI TR 03119. The BSI test seal can, after a successful certification and following the terms of usage specified by BSI, be placed on the card reader and be used for advertising purposes.

If a certification according to BSI TR 03119 is a prerequisite for the official use of a card reader, the application of the BSI test seal is mandatory. This can also apply if such qualification is required for tendering or similar procedures.

For more information on the certification procedure according to Technical Guidelines, refer to the BSI website.

3 Categories of Smart Card Readers

For reasons of interoperability and as a basis for evaluation and assessment all smart card readers have the same basic properties. Depending on the application, different additional functionalities and hardware variants are required for the smart card readers.

Three categories of smart card readers are described in the following subsections (see 1).

3.1 Basic Reader (Cat-B)

Simple card readers are often generically developed, or they have been designed for a particular application and therefore support several basic functions, which can be used by applications with similar requirements.

	Reader Category			Module Appendix A	Test Specifications Appendix B
	Cat-B	Cat-S	Cat-K		
Interface to the host computer	X	X	X	A.1	B.1
Contactless interface according to [ISO 14443]	X	X	X	A.2	B.2
Contact interface according to [ISO 7816]	O	O	X	A.3	B.3
PIN pad (secure PIN entry) with PACE support	O	X	X	A.4	B.4
Display (2x16 alpha-numeric characters)	O	O	X	A.5	B.5
Qualified signature with contact cards	O	O	X	A.6	B.6
Qualified signature with contactless cards according to [TR-03117] (e.g. identity card)	O	O	X	A.7	B.7
Firmware update	O	X	X	A.8	B.8
	X = mandatory; O = optional				

Table 1: Overview of Smart Card Reader Categories

The Basic Readers (Cat-B) can be deployed for home use or can be a building block for integrated devices like smart phones or notebooks, amongst others for the following services:

- eGovernment services of the identity card (e.g. authentication service, pension insurance scheme)
- age verification
- eTicketing according to VDV core application (VDV – Association of German Transport Companies) with contactless smart card as specified for VDV core application.
- proof of identity and proof of residence for Internet shopping

For these applications the reader device supports the exchange of data between the carrier medium and the respective application server on the Internet.

3.2 Standard Reader (Cat-S)

One frequently finds smart card readers, which meet higher quality requirements, being designed such that they can be placed on the table and varying in form (e.g. with a PIN pad, display etc.) depending on the desired fields of application. These smart card readers are designated as Standard Readers here and have at least a PIN pad to ensure the secure PIN entry.

In addition to the applications for which a Cat-B reader is designed, a Standard Reader can be used for the following applications (depending on the characteristics):

- eID function on the Internet with increased security requirements
- (optional) contact interface applications
- (optional) qualified signature (requires confirmation according to the signature law).

3.3 Comfort Reader (Cat-K)

Another card reader variant is the Comfort Reader which can be used for a variety of applications due to its versatility and convenient utilisation modes. It has at least a PIN pad to allow secure PIN input and a display with 2 x16 alpha-numeric characters. The Comfort Reader supports all functions of the eID card, including the qualified electronic signature.

Next to the contactless interface e.g. of the identity card including the signature function, also the contact interface of classic signature cards or of health cards including security functions is supported. Support for bank applications (FinTS, Secoder) or other applications is also possible.

Whereas the Basic Readers constitute the inexpensive variant, used especially for applications with limited security level dedicated to home users, the Standard and Comfort Reader devices are, in addition, construed for applications with extended security functions in terms of both function and safety.

4 General Recommendations

This chapter contains general recommendations for the characteristics of a card reader. The recommendations are not binding and not a part of the conformity evaluation. The scope of the conformity evaluation for the individual modules is specified in the Appendix B.

4.1 Utilisation Processes and Use Cases

The specification of the devices must take all use cases in the life cycle of the smart card reader into consideration. The following specific features have to be taken into account:

1. The installation of the device is usually carried out by the user.
2. If the reader supports a firmware update and a firmware update proves to be necessary in the course of time, the update must be installed on the card reader by the end-user with the help of a simple procedure.
3. In the course of time, application-specific software packages may be installed, depending on the choice of services which are to be used. This applies to the initial installation and to the updates.
4. In principle, concurrently using an arbitrary number of services provided by different suppliers should be possible.
5. As soon as a service is not needed any more, the service-specific software should be uninstalled.

4.2 Fundamental Requirements and Assumptions

All legal and other regulatory requirements always have to be met, such as EMC limiting values, the CE label or waste disposal commitments according to EU policies.

Different requirements and considerations should be taken into account when developing a smart card reader based on this guideline:

- **Optimising the cost-benefit ratio**: Depending on the designated use, different equipment characteristics are necessary, one has to weigh the pros and cons relevant for the application when considering, for example, the costs and benefits of a PIN pad or a display.
- **User friendliness**: Also laymen must be able to easily install the card reader at their PC. This concerns particularly the Basic Readers.
- **Fault tolerance**: At failure of hardware components which can be diagnosed regarding the logic of the card reader, the smart card reader should not assume an undefined status but react with termination and/or error messages.
- **Support**: In the case of technical problems the user must have a possibility to perform a simple check of his smart card reader and – should he need further support – technical customer support must be available.
- **Operating systems**: To prevent unnecessary constrains to the users, as many operating systems as possible shall be supported, i.e. corresponding drivers must be available including the necessary updates.
- **Security of the PIN pad**: Provided that the reader is equipped with a PIN pad, the design of such must ensure its security. This means that e.g. the PIN entered must neither be transferred to the host nor to the card in an unprotected way (particularly if a contactless interface is used).
- **Security of the display module**: An integrated display – if available – shall be used to provide the user with information securely. In the case of the eID function of the identity card, the displayed data comprise e.g. the access rights and the name of the provider.
- **Cryptographic procedures**: If cryptographic procedures are implemented for the card reader (e.g. PACE), these procedures must be implemented in a secure way. This concerns both the correct and secure implementation of the cryptography itself and e.g. the secure generation of key material (random numbers).

- **Protection against manipulation**: The end-user should be able to recognize that the device has not been manipulated. This particularly refers to card readers with built-in security functions, such as PIN pad or keyboard.
- **Conformity Testing**: If further applications are supported, e.g. gematik applications (electronic health card), VDV core application or banking applications, it is recommended to test the interoperability according to the respective standards. These tests are not subject of this guideline.

These requirements should be taken into account when selecting the function modules and their implementation.

4.3 Interfaces

A smart card reader serves as the link between the chip card, the host computer and the user, and respectively provides interfaces to at least these three entities. If interfaces beyond the modules defined in appendix A are implemented, BSI recommends testing these interfaces based on the corresponding test specifications.

4.3.1 Smart Card Interface

Appendix A contains definitions of modules for the contactless interface according to [ISO 14443] and for the contact interface according to [ISO 7816] as basic card reader interfaces in compliance to this guideline.

4.3.1.1 EMV Support

Banking applications can optionally be supported. The essential requirements are laid down in the [EMV] standard. Since this standard is not compatible to [ISO 7816], a switchover option can be provided in the smart card reader controlled by the application on the host computer if both standards are to be supported. In this case, the mechanism for switching between EMV mode and ISO mode has to be described by the manufacturer in the instruction manual or the programming manual.

4.3.1.2 Synchronous Smart Cards

Next to asynchronous chip cards, synchronous chip cards can also be used with the contact interface.

If after positioning a contact smart card for reading, the card reader does not receive an ATR as specified in [ISO 7816] part 3, it will be assumed that there is a synchronous card in the contact unit. The smart card reader thereupon initiates an activation of the smart card according to the conventions for synchronous chip cards. The card reader interprets the first 32 clock cycles as a 4 byte long ATR of a synchronous smart card as specified in [ISO 7816] part 10, and if successful, it determines the protocol for data transmission to be used with the card correspondingly. On failure, the smart card reader tries to establish the communication with the chip card without the reset function using the I²C bus protocol. If this is not successful either, the contacts are deactivated in accordance with the requirements of [ISO 7816] part 3.

4.3.2 Interface to the Host Computer

The fundamental interface between the card reader and the host computer is PC/SC or CCID (see module A.1). Additionally, other interfaces can be supported, e.g. [MKT] (Multifunktionales Kartenterminal) for synchronous cards used in the health care sector.

4.3.3 User Interface

Smart card readers can employ a variety of user interfaces. The PIN pad and the display are specified within the modules in A.4 or A.5 respectively.

If a PIN pad is available, the following regulations should be followed:

- In a 12 key input device, the 11th and 12th key should be assigned respectively to the Cancel and Confirmation functions;
- If a 16 key input device is used, an additional correction key should be provided.

Care should be taken to provide an ergonomic form of the keyboard and a barrier-free access for people with disabilities e.g. by using a tactile key field or text in Braille. The layout of the keys can be based on [CEN 1332] part 5.

Furthermore, the card reader can offer further user interfaces, some of them are listed as examples in the following.

4.3.3.1 LEDs

The smart card reader is ready to use after connecting the supply voltage. An light-emitting diode in a first colour (preferably green) indicates the state after a correct initialisation of the card reader. The operating mode after activation (contact) or selection (contactless) of the chip card is indicated by an LED if possible in a second colour (preferably yellow). Should there be a differentiation between interfaces, yellow should be reserved for the contact interface and blue for the contactless one. A blinking LED in the second colour or a third colour signalises a failure. The exact behaviour of the LED has to be described in the user manual.

At least one LED display should be present. It shows as a minimum if a chip card is currently activated or selected. Also the user should be able to see that the card reader is ready.

Exceptions can be made if the design of the reader (e.g. integrated smart card reader) offers no possibilities to integrate any LEDs.

4.3.3.2 Indication of the Secure Mode

Security-relevant applications require authentic input and output.

For example, an indicator is provided to tell a user that the secret number entered using the keyboard of the smart card reader will not be transmitted into the insecure environment of the PC used or into the host computer via insecure communication channels. Also output pertaining to e.g. a digital signature or a payment procedure may require an indication of authenticity.

The information that the smart card reader is in the secure mode has to be conveyed to the user in an explicit way. For this purpose, acoustic, visual or other clearly perceptible signals can be used. Common indicators used at present are additional LEDs or symbols appearing in the display. It should be taken into account that a barrier-free support of the function is available, e.g. by using enlarged symbols or a combination of visual and acoustic signals.

It has to be ensured that the signal cannot be accessed in an unauthorized way and is only controlled by the firmware residing on the smart card reader.

The usage of such signals must be documented in the user manual in an unambiguous way.

4.3.3.3 Biometric Sensor

The smart card reader can additionally have one or more biometric sensors. Possibilities include for instance fingerprint, speech recognition or iris scanning for the identification of biometric characteristics.

The biometric data must not be transmitted in the environment of the host computer.

No further criteria relating to the function and security of the biometric systems are specified in this guideline.

A Modules

The following modules serve to ensure the interoperability and compatibility of different smart card readers. Combinations of mandatory and optional modules will determine different types of readers, hence not all modules have to be taken into account in every card reader.

Also, the reader can have properties or support functions, which are not defined in any of the following modules. However, if the type or the function unit is defined here, exclusively the subsequent module descriptions shall be used.

If commands for controlling the card reader are required (e.g. PIN input), no proprietary commands shall be used, only the terminal commands specified here.

A.1 Interface to the Host Computer

A.1.1 Supported Operating Systems

Depending in the card reader type, the following Operating Systems must be supported by the card reader/the corresponding driver:

- An *External Smart Card Reader* is a separate device and connected to the host computer via e.g. USB. An External Smart Card Reader must support at least the following Operating Systems:
  - Windows; MacOS X; Linux (e.g. Debian, Ubuntu, openSUSE).
- An *Integrated Smart Card Reader* is a device integrated into the host computer, e.g. a notebook. The card reader must support the following Operating Systems, as far as they are available for the host computer. For each Operating System from the list, which cannot be supported, the technical impossibility or the legal non-admissibility of supporting this Operating System must be justified.
  - Windows; MacOS X; Linux (e.g. Debian, Ubuntu, openSUSE).
- An *Embedded Smart Card Reader* is a card reader integrated into an embedded device, e.g. a smart phone. Embedded devices do not allow the installation of different Operating Systems, therefore in this case the Operating System of the embedded device must be supported.

At least one version of each Operating System, being supported by its vendor at the time of certification, must be supported. If both 32 bit and 64 bit versions are available, both must be supported. The supported Operating Systems must be clearly indicated by the manufacturer of the card reader.

An update of the interface drivers for future and further versions of the Operating Systems must be possible and be provided by the manufacturer on demand.

A.1.2 API

Depending on the Operating System, at least one of the following APIs must be supported by the card reader/the driver of the card reader:

- **PC/SC**: The communication with the card reader is carried out via [PC/SC]. PC/SC is a standard for accessing smart card readers, developed by the PC/SC Workgroup. For PC/SC on Windows platforms, WHQL certificates by Microsoft are necessary. If applicable, the PC/SC mapping for commands from Appendix D is used.

- **CCID**: CCID is a USB driver class for smart card readers specified in [CCID]. The reader must support transmission and receiving of extended APDUs as defined in [CCID]. If applicable, the CCID mapping for commands from Appendix D is used.

As a special case, embedded card readers are accessed using the applicable methods of the Operating System, e.g. on Android the class `android.nfc.tech.IsoDep` is used for communication with embedded card readers. If applicable, the CCID mapping for commands from Appendix D is used.

While PC/SC allows more flexibility, especially in a multi-application environment, CCID allows the construction of card readers without dedicated software driver, i.e. driverless installation. The choice of supported interfaces is up to the card reader vendor. Therefore a client application must support both interfaces. If a card reader supports both interfaces, the client application should use the PC/SC interface.

A.1.3 Information about the Reader

The smart card reader (or the driver of the reader) must provide commands to retrieve the following information:

- vendor name
- product designation
- firmware version
- driver version.

The commands are listed in Table 2.

Command	Description
0xFF-0x9A-0x01-0x01-0x00	vendor name
0xFF-0x9A-0x01-0x03-0x00	product name
0xFF-0x9A-0x01-0x06-0x00	firmware version
0xFF-0x9A-0x01-0x07-0x00	driver version[2]

Table 2: Command Overview GetReaderInfo

Example:

Command: 0xFF-0x9A-0x01-0x07-0x00

Response: 0x31-0x2e-0x30-0x31-0x90-0x00 („1.01“)

These commands have to be implemented for all interfaces. However, they only have to be provided when a smart card is available at the respective interface. The implementation of this functionality without a card being available is optional.

A.2 Contactless Interface

Contactless smart card readers meet the requirements according to [ISO 14443] parts 2, 3 and 4[3].

The card reader supports protocol types Type A and Type B according to [ISO 14443] part 2.

2 If the card reader is supported by Operating Systems listed in A.1.1 without a driver and no drivers are delivered with the card reader, the string „CCID“ shall be returned as the driver version.

3 Note: In accordance to the current version of [ISO 14443] part 2, this means in particular a minimum field strength of 2A/m for the field generated by the reader. Further, this includes mandatory support for Extended Length APDUs (“I-block chaining”) according to [ISO 14443] part 4.

The following transmission protocol is supported as a transport layer protocol:

- T=CL, block-oriented half-duplex protocol according to [ISO 14443] part 4, including „Protocol and Parameter Selection“ (PPS).

At least data transfer rates of 106, 212 and 424 kbit/s as specified in [ISO 14443] part 2 must be supported.

For the contactless interface, the card reader must support cards in the format td1 (85,6 mm x 54.0 mm x 1.25 mm) compliant to [ICAO 9303] part 3, volume 1, though supporting a card thickness in the range from 800µm to 1100µm is sufficient (card thickness 800µm to a maximum of 900µm; address label with lamination to a maximum of 200µm). The format td1 implies a Class 1-antenna according to [ISO 14443] part 1.

If a contact interface is supported (module A.3), upon switching from a contact card to a contactless card a reset is necessary with an ATR conforming to [ISO 7816] part 3, sent to the application.[4] This is specified in [PC/SC] part 3.

A.3 Contact Interface

Multifunctional reader types can additionally support contact smart cards. Such readers have at least one contacting unit for smart cards of size ID-1 (85.6 mm x 54.0 mm x 0.80 mm) in accordance with [ISO 7810]. If the same slot is used for the contactless interface according to module A.2 and the contact interface, special attention must be paid that the contacting unit does not damage cards of the format td1 (see also module A.2). Should different card slots be used and the contact slot is unsuitable for cards of the format td1, the instruction manual for the reader has to point this out explicitly.

The dimensions and location of the electrical contacts are specified in [ISO 7816] part 2. Furthermore, the smart card reader can have additional optional contacting units. They can be designed also for the format ID-000 (plug-in card) according to [ISO 7810].

The contacts of the smart card reader must be resistant against short circuits of individual contacts or all contacts together. After a short circuit between the contacts, all functions of the card reader must be completely recoverable. No irreversible damages may occur.

Note that some dual interface smart cards have a combined power management for the contactless and the contact interface. Therefore the contact pads of a dual interface card must not be shorted or connected to GND if the contact interface is not in use.

The card reader provides the smart card with the supply voltage of 5 V as standard for Class A according to [ISO 7816] part 3. The support for an additional lower supply voltage for power saving is optional. This corresponds to Class B and Class C for 3 V and 1,8 V smart cards, respectively, according to [ISO 7816] part 3.

The operation of asynchronous contact smart cards with the card reader is undertaken in a way conforming to [ISO 7816], part 3. It comprises:

- activation of the smart card
- behaviour and configuration during ATR (“answer to reset”)
- Protocol and Parameter Selection (PPS)
- information exchange with the smart card
- deactivation of the smart card

4 Note: According to [TR-03110] the security status of an identity card can be reset by SELECT MF without Secure Messaging. This is not supported by all eID cards (cf. [TR-03127]). For these cards, a reset of the security status after an executed authentication is only possible by switching the reading field off and on. This can be supported by the smart card reader using the PC/SC command SCardReconnect with SCARD_RESET_CARD or the CCID command PC_to_RDR_IccPowerOn. No signal identifying a new card should be sent to the host computer.

The support of PPS and the selection of protocol and parameters pertaining to it, is required to achieve higher data transfer rates in accordance with [ISO 7816] part 3.

After a smart card is positioned for reading, it is assumed at first that an asynchronous smart card is to be read. A reset command sent to the card reader executes an activation sequence and an evaluation of the ATR ("Answer to reset") according to [ISO 7816] part 3. In the case of missing or incorrectly received ATR of an asynchronous card, the card reader can repeat the activation twice as a maximum.

The following transmission protocols are supported:

- T=1, block-oriented half-duplex protocol according to [ISO 7816] part 3
- T=0, character-orientated half-duplex protocol according to [ISO 7816] part 3.

A.4 PIN Pad Supporting PACE

The smart card reader can possess a keyboard. In this module, the requirements for a PIN pad will be defined (including the requirements resulting from supporting PACE).

A.4.1 Secure PIN Input

The PIN will be transmitted directly from the keyboard of the card reader to the smart card, the data does not leave the terminal. The verification of the PIN takes place in the card. A higher level of security for the PIN is achieved this way, in comparison with card readers without a PIN pad. For the latter, there is always a possibility that e.g. a keylogger on the host computer also reads the PIN.

A contactless smart card reader uses the PACE protocol to protect the data communication via the contactless interface.

If, next to the secure PIN input, the reader supports a non-secure PIN input (e.g. a PIN input at the host computer for certain applications), this must be conveyed to the user in an explicit way (cf. also 4.3.3.2). A non-secure PIN input can be provided only for applications, where corresponding specifications prescribe it. The signalling must not be controllable by the host computer.

An entered PIN has to be immediately deleted or overwritten after use.

A.4.2 PACE

The PACE protocol allows for establishing a secure channel between the reader device and the smart card. When a reader with a PIN pad is used, PACE is executed directly in the card reader.

For this module, PACE support with Capabilities PACE and eID according to Appendix D must be implemented.

The card reader must be capable of employing the cryptographic algorithms and key lengths according to [TR-03116] part 2. For reasons of future reliability, it may be useful to also support other key lengths. The requirements from [TR-03116] part 2 on random numbers for key generation must be met.

A.4.3 PIN Management

Changing the eID-PIN is performed by a verification of the existing eID-PIN using the method EstablishPACEChannel(Password=eID-PIN, Role=unauthenticated) and subsequent setting a new eID-PIN with the help of ModifyPIN according to Appendix D.

In order to query the retry counter of the eID-PIN, the command MSE:SetAT is used in the coding for the start of the PACE protocol in the role of an unauthenticated terminal. The reader device must ensure that the

host computer can query for the retry counter using this command, but cannot execute the complete PACE protocol.

The method EstablishPACEChannel(Password=PUK, Role=unauthenticated) with a subsequent RESET RETRY COUNTER has to be supported to perform a reset of the retry counter.

A.4.4 Filtering Rules

To prevent circumvention of the secure PIN input using the PIN pad, the card reader must filter certain commands, i.e. it must not execute or must not forward the commands to the card. This means:

- It must be prevented that PACE can be executed by the host computer.
- EstablishPACEChannel must not be performed with an eID-PIN or PUK provided by the host computer, the input of these secret codes exclusively at the PIN pad must be enforced.
  If EstablishPACEChannel is used with CAN provided by the host computer, the card reader must request a user confirmation before establishing the secure channel.
- The following combinations of role-and-password pairs must be supported:
  - "unauthenticated terminal" with CAN, PUK and eID-PIN
  - Authentication Terminal with CAN and eID-PIN
  - if module A.7 (QES with contactless cards) is implemented: Signature Terminal with CAN, eID-PIN and PUK.

  All other combinations must be filtered out.
- It must be prevented that the eID-PIN can be changed by the host computer (RESET RETRY COUNTER).

Additional filtering is permitted as long as it does not affect the functionality of the reader device.

A.4.5 Protection against Manipulation

The PIN pad must be designed in a way allowing for effective prevention of a PIN pad manipulation or allowing the owner to recognise that manipulation took place. The necessary protection level must be based on the specifications of the signature law.

A.5 Display

A display must contain at least 2 lines with a minimum of 16 display characters in each line.

As a character set, upper- and lower-case letters including the umlaut and special characters must be supported as specified in DIN 66003. Besides the German language, other languages to display messages can be implemented. Further symbols and characters for the user interface (e.g. secure mode) are permitted.

A blinking cursor symbol should show the position of the cursor when texts are displayed requiring a subsequent keyboard input.

The following standard texts must be provided in the card reader. The semantics of the texts are binding, the specific wording can differ.

No.	*Text (German, mandatory)*	*Text (English, optional)*
1	`Bitte Karte bereitstellen`	`Please insert / position card`
2	`Bitte Karte entfernen`	`Please remove card`
3	`Karte unlesbar. Falsche Lage?`	`Card unreadable. Wrong position?`
4	`Bitte Geheimzahl eingeben`	`Please enter secret number`
5	`Aktion erfolgreich`	`Action successful`
6	`Geheimzahl falsch/gesperrt`	`Secret number incorrect/locked`
7	`Neue Geheimzahl eingeben`	`Enter new secret number`
8	`Eingabe wiederholen`	`Repeat entry`
9	`Geheimzahl nicht gleich. Abbruch`	`Secret numbers differ. Cancel`
10	`Bitte Eingabe bestätigen`	`Please confirm input`
11	`Bitte Dateneingabe`	`Please enter data`
12	`Abbruch`	`Cancel`
If for texts no. 4, 6, 7, 9 additional information on the type of the secret number (PIN, PUK, …) is available, the displayed text should indicate the type of the number.		

Table 3: Standard Display Texts

The card reader must indicate in a clear way, whether the displayed information is authentic and generated by the reading device itself or controlled by the host computer (cf. also 4.3.3.2).

A.5.1 Use of eID

The card reader must ensure the authentic display of the certificate holder and access rights before the user enters his PIN. The name of the certificate holder must be retrieved from the certificate description, the access rights from the CHAT. transmitted by `EstablishPACEChannel`.

For this module, PACE support with Capabilities PACE and eID according to Appendix D must be implemented.

In order to provide a consistent user guidance for the eID, the following standardized display texts shall be used after the process is initiated by the host (`EstablishPACEChannel`):

	Text	
	German, mandatory	***English, optional***
If no card is present	`Bitte Karte einlegen`	`Please insert card`
To display the holder of the authorization certificate	`Zugriff durch:` <*name from cert desc*>	`Access by:` <*name from cert desc*>
To display the access rights as transmitted in the CHAT	`Zugriff auf:` <*see below*>	`Access to:` <*see below*>

The access rights shall be denoted by these texts. The texts can be either displayed seperately (the user has to confirm each right) or as a batch, e.g. using scrolling text. In the latter case the user should be able to adapt the scrolling speed.
The texts are abbreviated to fit into a 16-character display. If a larger display is available or scrolling texts are used, the texts may be used in the corresponding unabbreviated form.
	`Dokumentenart`
	`Ausstell. Staat`
	`"Gültig bis"`
	`Vorname(n)`
	`Familienname`
	`Ord./Künstl.name`
	`Doktorgrad`
	`Geburtsdatum`
	`Geburtsort`
	`Staatsangehör.`
	`Geburtsname`
	`Anschrift`
	`Nebenbest.`
	`Pseudonym`
	`Wohnortbestät.`
	`Altersbestät.`
		`Document type`
		`Issuing country`
		`"Valid until"`
		`Given name(s)`
		`Family name`
		`Rel./art. name`
		`Doctoral degree`
		`Date of birth`
		`Place of birth`
		`Nationality`
		`Birth name`
		`Address`
		`Aux. conditions`
		`Pseudonym`
		`Address verif.`
		`Age verification`

The special case of installing a signature certificate should always be displayed seperately.	`Sign.-Zertifikat installieren`	`Install sign. certificate`

These identifiers shall be used to denote the different secrets.	`PIN`
	`PUK`
	`Zugangsnummer`
	`Signatur-PIN`
		`PIN`
		`PUK`
		`Access number`
		`Signature PIN`

To ask the user to enter a secret, this text shall be used.	<*secret*> `eingeben`	`Please enter` <*secret*>
During execution of PACE	`Überprüfe` <*secret*>	<*secret*> `verification`
After successful execution of PACE	`Verbindung aufgebaut`	`Connection active`
If PACE failed because the entered secret is wrong	<*secret*> `falsch`	<*secret*> `not correct`
If PACE failed because the secret is blocked	<*secret*> `gesperrt`	<*secret*> `blocked`
If PACE failed because the PIN is deactivated	`eID nicht aktiviert`	`eID not activated`
During reading of data by the host	`Lese Daten`	`Reading data`

A.5.2 Protection against Manipulation

The display must be designed in a way allowing for effective prevention of display manipulation or allowing the owner to recognise that manipulation took place. The necessary protection level must be based on the specifications of the Signature Law/Signature Ordinance.

A.6 QES with Contact Cards

The reader device must adhere to the specifications of the Signature Law and Signature Ordinance.

A.7 QES with Contactless Cards according to TR-03117

This module defines the protocols and reader properties necessary for the generation of qualified signatures with contactless cards according to [TR-03117] (e.g. the German identity card). The generation of a qualified key pair or loading a qualified certificate is carried out in the role of an authentication terminal, thus it is not in the scope of this module.

The card reader must implement the reader-side of the protocols described in the following subsections. The detailed process is described in [TR-03110] and [TR-03117].

For this module, PACE support with Capabilities PACE and eSign according to Appendix D must be supported.

The card reader must be capable of employing the cryptographic algorithms and key lengths according to [TR-03116] part 2. For reasons of future reliability, it may be useful to support additional key lengths.

A.7.1 PACE

The card reader must support PACE with the Card Access Number (CAN) as password. The CAN can be entered either via the PIN pad of the reader or be already known to the reader (i.e. stored in the reader or the signature creation application).

A.7.2 Terminal Authentication

For access to the signature function the card reader identifies itself to the card via Terminal Authentication as a confirmed signature terminal. In order to perform the Terminal Authentication the reader must possess a private key and be able to generate a signature with this key. The corresponding public key must be signed by the DV-eSign of the EAC PKI.

The certification of the readers by the DV-eSign is carried out as part of the confirmation of the model type certification, i.e. all readers of the same (confirmed) construction type receive the same certificate and the same private key. This key is generated by the vendor and stored in a secure way. The secure storage as well as secure transport of the key into the reader is part of the evaluation for obtaining the confirmation. After a successful confirmation of the reader type, the public key will be certified by the DV-eSign (located at the BSI).

For a re-certification the manufacturer sends a new certificate request for the already existing private key to the BSI. The prerequisite for a renewed certification is the continued validity of the confirmation of the reader and the sufficient key length of the private key according to [TR-03116] part 2.

If the key length does not suffice any more, there are two possibilities:

1. During the production process multiple private keys of various lengths are stored in the reader, of which one is suitable for the re-certification.

2. The reader is capable of importing a new key using a secure interface.

For more details on the certification by the DV-eSign refer to [CP-eSign].

A.7.3 Passive Authentication

The card reader reads the file EF.CardSecurity and verifies the signature contained in it. For the signature validation a chain of certificates has to be examined, ending at the CSCA certificate of the BSI. The card reader has to store the CSCA certificate in a manipulation-proof way. All other necessary data and certificates are stored on the identity card itself.

When the BSI changes the CSCA certificate (about every 2-3 years), the new certificate must be made available to the reader and stored in the reader for signature validation. A secure import of the certificate is not necessary, since the new certificate can be verified using the old root certificate. The specifications of the key lengths according to [TR-03116] part 2 must be taken into account.

A.7.4 Chip Authentication

Using the public key of the chip retrieved from the file EF.CardSecurity and verified with the help of the Passive Authentication, a new secure channel (Secure Messaging) between the reader and the identity card will be established, which replaces the PACE channel.

A.7.5 Signature PIN

In order to use the signature PIN, the card reader must implement the following procedures using the commands from Appendix D, and translate them in the corresponding commands/command sequences according to [TR-03117].

- Verifying the signature PIN is triggered by the host computer using VerifyPIN. This command may be used on the contactless interface only after a successful execution of EstablishPACEChannel(Password=CAN, Role=SignatureTerminal).
- Changing the signature PIN is triggered by ModifyPIN. This command may be used on the contactless interface only after a successful execution of EstablishPACEChannel(Password=CAN, Role=SignatureTerminal).
- Setting a new the signature PIN is triggered by ModifyPIN. This command may be used on the contactless interface only after a successful execution of EstablishPACEChannel(Password=eID-PIN, Role=SignatureTerminal).
- Resetting the retry counter is performed using the command CHANGE REFERENCE DATA according to [TR-03117] after an execution of EstablishPACEChannel(Password=PUK, Role=SignatureTerminal).

A.7.6 Filtering Rules

Setting/changing/using the signature PIN can be performed only using the described commands, this means in particular that the card reader must filter the commands of the host computer accessing the signature PIN (especially VERIFY and CHANGE REFERENCE DATA).

A.7.7 Signature Generation

The generation of the signature is performed using standard commands according to ISO 7816, as specified in [TR-03117].

A.8 Firmware Update

If a card reader supports updates, the card reader must be equipped with a secure firmware download function. The firmware of the smart card reader is the fundamental basis for securing the approved service features.

The download function can be executed with a separate loading program, which is provided for the various system environments.

If the firmware provides security services (i.e. if the reader implements any of the modules A.4 – A.7), the download process must be protected in the way preventing that the reader firmware can be modified by an unauthorised access. By using a cryptographic securing system it must be guaranteed that only authorised persons or systems can change the features of the smart card reader. The integrity and completeness of the new data must be verified by the firmware of the reader itself. Protecting the data using a digital signature is mandatory.

B Certification Requirements

This appendix describes the testing requirements for the respective modules defined in Appendix A. The test reports or manufacturer's declarations are to be presented to the BSI certification authority in the course of the certification procedure.

To verify the correct functional implementation of the modules, functional tests and conformity tests are carried out.

If the reader supports a security-relevant module (modules form A.4 up), the security must be proven by a Common Criteria certification as specified in Appendix E. Depending on the module, additional specific requirements must be met, e.g. a confirmation according to the Signature Act. The individual types (model, PIN, biometrics, displays, etc.) determine the scope of the evaluation.

B.1 Interface to the Host Computer

The functional tests ascertain the interoperability among diverse smart card readers and verify the basic requirements by practical testing. All functional tests performed must be documented in a test report.

Testing the reader devices comprises:

- the installation of a smart card reader including the driver on the Operating Systems according to A.1.1 and
- the functional tests including verification of the driver interface on these Operating Systems.

The tests to be performed are described in the Appendix C and have to be conducted by a test lab recognised by BSI according to DIN ISO/IEC 17025 for the performance of conformity evaluations according to [TR-03105].

B.2 Contactless Interface

The manufacturer of the smart card readers has to prove that use of smart cards of the format td1 (up to a thickness of 1100µm, cf. A.2) with the contactless interface does not cause any damage.

For all reader types, the conformity to [TR-03105] part 4, has to be proven. For this purpose, a conformity evaluation for the ISO Layer 2-4 has to be performed by an evaluation facility recognised by BSI according to DIN ISO/IEC 17025. All test reports of the conformity evaluation are to be submitted as proof of conformity.

B.3 Contact Interface

The contact interface has to be tested according to [ISO 10373] part 3. The examination must be performed by an evaluation facility recognised by BSI according to DIN ISO/IEC 17025. Alternatively, verifications according to [EMC] together with supplementary testing according to [ISO 10373] can be performed. The detailed scope of the testing will be determined by the BSI.

B.4 PIN Pad with PACE Support

For validation of the PACE implementation, a conformity evaluation of the ISO Layers 6-7 according to [TR-03105] part 5.2 has to be performed by a test lab an evaluation facility recognised by the BSI according to DIN ISO/IEC 17025. At least the tests of the profiles R_Tra, R_PACE and R_eID have to be performed.

The functions of the reader device declared in the manufacturer's Implementation Conformance Statement (ICS) can restrict the tests to be performed. The card reader must be capable of employing the cryptographic algorithms and key lengths according to [TR-03116] part 2. For reasons of future reliability, it may be useful to also support other key lengths

All test reports of the conformity evaluation are to be submitted as proof of conformity.

The adherence to the security policies, in particular:

- secure handling of the PINs entered, especially deletion of the PIN after use
- implementation of PACE (e.g. key generation)
- compliance to filter rules
- protection against manipulation
- if available: indication of the secure mode

have to be proven using a Common Criteria certification (see Appendix E). It is recommended to base the certification on the Standard Reader Protection Profile [PP-0083], which covers the listed security policies.

B.5 Display

The security of the display, in particular:

- authentic display, especially correct display of the certificate holder and the access certificates when using the eID function
- manipulation-proof display

has to be proven using a Common Criteria certification (see Appendix E).

B.6 QES with Contact Cards

A confirmation according to the Signature Law has to be presented.

B.7 QES with Contactless Cards according to TR-03117

A conformity evaluation of the ISO Layers 6-7 according to [TR-03105] part 5.2 has to be performed by an evaluation facility recognized by BSI according to DIN ISO/IEC 17025. At least the profiles R_Tra, R_PACE, R_TA, R_CA, R_eID and R_Sig have to be carried out.

The functions of the reader device declared in the manufacturer's Implementation Conformance Statement (ICS) can restrict the tests to be performed. The card reader must be capable of employing the cryptographic algorithms and key lengths according to [TR-03116] part 2. For reasons of future reliability, it may be useful to also support other key lengths

All test reports of the conformity evaluation are to be submitted as proof of conformity.

The security of specific mechanisms for use of the QES with contactless cards has to be proven by the following certifications:

- The private key for the Terminal Authentication must be stored in a secure way. For this purpose, a security module, certified according to [PP-SSCD] compliant to Common Criteria with Assurance Level EAL4+, must be used. In exceptional cases, other security modules can be used in accordance with BSI.
- The software accessing the security module (Firmware) must be certified with Assurance Level EAL 3, based on the Security Target of the vendor. It is recommended to create this Security Target based on the Protection Profile [PP-IS]. If the Security Target is not derived from this Protection Profile, it must be ensured that the corresponding security requirements are represented in the Security Target.
- If the optional import of a new private key for the terminal authentication is implemented, the import mechanism has to be certified at Assurance Level EAL4+. This is not covered by [PP-IS], thus it must be additionally considered in the Security Target.

A confirmation in accordance with the Signature Law must be presented.

B.8 Firmware Update

The security of the firmware updates, in particular:

- securing and verifying the integrity of the firmware

has to be proven by a Common Criteria certification, provided the firmware contains security-relevant components (see Appendix E).

C Functional Tests

The tests in this section verify the functionality of the card readers or respectively of the pertaining drivers for the supported Operating Systems (see Appendix A.1). The functional tests are not a substitute for the conformity evaluation according to [TR-03105].

C.1 General Requirements

To perform functional tests of reader devices, consistent, unchanging and reproducible test environments have to be created. The following sections describe the requirements for the test instruments as well as the necessary preparations for carrying out the tests.

C.1.1 Test Instruments

To perform the tests, various hardware and software components are necessary. In principle, the test setup should correspond to computer equipment utilised by a home user.

- Operating Systems listed in the Appendix A.1, each with the current patches of the OS vendor
- configured Internet access
- for each Operating System the current version of an eID-Client:
  - if the Operating System is supported by the AusweisApp, the up-to-date and officially available version of the AusweisApp[5] shall be used as eID-Client,
  - otherwise any other eCard-API compliant eID-Client may be used.
- nPA test card or nPA simulator

C.1.2 Preparations

To perform the test, a separate test system has to be set up for every tested Operating System. The installation of the various Operating Systems in a virtual machine is not permitted, since the connection to the card reader largely depends on the host system, which runs the virtual machine.

The installations of Windows and Linux Operating Systems can, in each case, be tested on the same hardware platform. For the test on the Operating System Mac OS, the hardware platform prescribed by the vendor must be used.

All Operating Systems must be updated to the most recent version using the updates provided by the OS vendor before the test is performed. The eID-Client has to be installed on the test computer.Moreover, a browser has to be configured for use with the eID-Client. For this purpose, an installation of a browser plug-in may also be necessary.

The installation of the drivers for the reader device is one of the test procedures.

C.2 Tests

All tests listed here must be performed for each of the Operating Systems listed in the Appendix A.1.

C.2.1 Installation Tests

The installation of the reader device is carried out following the installation guide – if available – provided by the manufacturer. If no instruction is enclosed with the reader, the installation is performed by connecting the reader to the system and subsequent installation of the device drivers using conventional installation methods. These have to be documented in the test report.

The reader device will be connected to the test system as described in the installation guide provided by the manufacturer. If additional software (made available by the vendor of the reader devices or a third party) must be installed prior to connecting the reader device, such software must be installed beforehand, as described by the vendor of the reader device.

If, after connecting to the test system, the reader device is automatically detected by the Operating System as a recognised device, the drivers recommended by the manufacturer are still to be installed.

In most cases *Embedded Smart Card Readers* do not need to be installed manually. Therefore, for these devices no installation tests are required.

5 Source: https://www.ausweisapp.bund.de

Errors caused by incorrect, missing or incompatible components of the Operating System (e.g. missing package dependencies in Linux systems) are to be analysed and documented.

C.2.2 Functional Tests

For the following tests, a successfully installed reader device is a prerequisite. All tests described here have the objective to verify the functionality of the reader device in the interaction with the eID-Client. Depending on the modules from Appendix A used in the reader, the test procedure differs only slightly. Vendor-specific additional software will not be tested.

Instead of a test card, a corresponding simulator for performing reader tests can also be used. This can minimise the test overhead as the state of the card (suspended, blocked) can be directly simulated.

When testing reader devices with a display, one must ensure that the formulated messages from Chapter A.5 are used and correspond in each case to the functions of the respective test.

C.2.2.1 Card Recognition

After positioning the test card on the reader to be tested, eID-Client will signal that a card has been recognised.

Preconditions

- No preparation necessary

Execution

- The card will be placed in the reading position defined by the manufacturer of the reader.

Documentation

- It must be documented, whether the card has been recognised and displayed in the eID-Client.

C.2.2.2 Reader Information

It will be verified if the reader supports retrieval of the reader information (see Chapter A.1.3).

Preconditions

- No preparation necessary

Execution

- All four commands from the Chapter A.1.3 Table 2 are to be successively sent to the reader device. In the response, the information requested in the string format and the status word 0x9000 is expected .

Documentation

- All return values are to be documented.

C.2.2.3 Changing PIN

Using the eID-Client the PIN of the test card is to be changed.

When using a reader device with a PIN pad, the PIN must be entered via this PIN pad. A prompt for the PIN via a PC keyboard is for this reader device not permitted. If a prompt for the PIN appears at the test computer, the PIN can still be entered only using the PIN pad of the tested reader device. Feedback of the PIN entered at the PIN pad to the test computer is not permitted.

When using reader devices with a display, the prompt for PIN input has to appear on this display.

Preconditions

- The card will be placed in the reading position defined by the manufacturer of the reader.

Execution

- In the eID-Client changing PIN will be invoked.
- The PIN will be set to a new value.
- After a successful change the PIN is to be changed to the original value.

Documentation:

- Feedback to both changes of the PIN is to be documented.
- In addition, it must be documented whether the PIN was entered using a PC keyboard or the PIN pad of the reader device.

C.2.2.4 CAN Input

The card must be put in the state “suspended” (see [TR-03110]). The reader device or the eID-Client respectively must prompt the user for entering CAN.

When using a standard or comfort reader, the PIN has to be entered at the PIN pad. A prompt for the PIN via a PC keyboard is for this reader type not permitted.

When using reader devices with a display, the prompt for PIN and CAN input has to appear on this display.

Preconditions

- The card will be placed in the reading position defined by the manufacturer of the reader.
- The card must be put in the status “suspended” (see [TR-03110]).
  A possible approach: In the eID-Client, select the option Change PIN. Repeat entering incorrect PIN until you will be prompted for CAN.
  Alternatively, a simulator can be used which can directly simulate this status.

Execution

- The correct CAN will be entered. If the eID-Client offers entering the CAN directly in the application for reader devices with a PIN pad, the input of the CAN both at the PIN pad and via the eID-Client should be tested.
- The correct PIN will be entered. When using readers with a PIN pad, entering PIN must be possible only directly at the reader.

Documentation

- The prompt for CAN and PIN input as well as the feedback of the reader device and eID-Client are to be documented.
- In addition, it must be documented whether the PIN or respectively the CAN was entered using eID-Client or the PIN pad of the reader device.

C.2.2.5 PUK Input

The card must be put in the state “blocked” (see [TR-03110]). After that the correct behaviour prompting for and allowing to enter PUK of the reader device is to be verified.

When using a reader device with its own PIN pad, the PIN and PUK must be entered on this PIN pad. A prompt for the PIN or PUK via a PC keyboard is not permitted for this reader device type.

When using reader devices with a display, the prompt for PIN, CAN or PUK input has to appear on this display.

Preconditions

- The card will be placed in the reading position defined by the manufacturer of the reader.
- The card must be put in the status "blocked" (see [TR-03110]).
  A possible approach: In the eID-Client, select the option Change PIN. Entering the PIN incorrectly several times will put the card in the state "suspended". The correct CAN will be entered and subsequently again the wrong PIN will be entered. The card will now be in the state "blocked".
  Alternatively, a simulator can be used which can directly simulate this status.

Execution

- To unblock the card, the corresponding function is to be invoked by the eID-Client. After entering the correct PUK, the original PIN is active again.

Documentation

- The display, the input procedures and the feedback of the reader device as well as of the eID-Client are to be documented.

C.2.2.6 Online Authentication

Within this test, the complete authentication at an Online portal has to be performed.

When using a reader device with a PIN pad, the PIN must be entered at this PIN pad. A prompt for the PIN via a PC keyboard is not permitted for this reader device type.

When using reader devices with a display, the prompt for PIN input has to appear on this display. Also, the display should show data of the authorisation certificate.

Preconditions

- The card will be placed in the reading position defined by the manufacturer of the reader.
- In a browser, the login page of a service provider supporting nPA login will be opened.

Execution

- In the service portal a login procedure will be started.
- In the case of reader devices with a display, the data in the display must correspond with the data in the authorisation certificate shown by eID-Client.
- The login procedure will be completed and the user authenticated by the correct input of the PIN. In the case of a reader device with a PIN pad, entering the PIN is only possible directly at this PIN pad. Entering the PIN directly in the eID-Client shall only be possible with reader devices without own PIN pad.
- A successful login is verified by inspection of read data accessible within the portal.

Documentation

- The service portal used is to be documented.
- The display, the input procedures and the feedback of the reader device as well as of eID-Client are to be documented.
- The feedback of the service portal after the login procedure is to be documented.

C.2.3 Filter rule Tests

For the following tests, a successfully installed reader device is a prerequisite. All tests described here have the objective to verify the correct behaviour of the reader device filter mechanisms (see chapter A.4.4). These tests have to be performed only for reader devices with PIN pad. For the test execution it may be necessary to use additional test tools on the host.

C.2.3.1 PIN/PUK filter

The command EstablishPACEChannel must not be performed with an eID-PIN or PUK provided by the host computer, the input of these secret codes exclusively at the PIN pad must be enforced. (see chapter A.4.4).This test has to be performed with PIN and PUK in separate test runs.

Preconditions

- The card will be placed in the reading position defined by the manufacturer of the reader.

Execution

- Initiate PACE with PIN/PUK. The PIN/PUK must be send inside the EstablishPACEChannel command direct to the reader device. The user should not be prompted to enter the PIN/PUK via the PIN pad.
- The card reader must deny the PACE establishment.

Documentation

- The display, the input procedures and the feedback of the reader device as well as the used test tool are to be documented.

C.2.4 CAN confirmation

If EstablishPACEChannel is used with CAN provided by the host computer, the card reader must request a user confirmation before establishing the secure channel (see chapter A.4.4).

When using a reader device with a PIN pad, the use of the CAN must be confirmed at this PIN pad. A user confirmation via the host PC is not permitted for this reader device type.

When using reader devices with a display, the prompt for CAN confirmation has to appear on this display.

Preconditions

- The card will be placed in the reading position defined by the manufacturer of the reader.

Execution

- Initiate PACE with CAN. The CAN must be send inside the EstablishPACEChannel command direct to the reader device. The user should not be prompted to enter the CAN but must be requested to confirm the use of the CAN via the PIN pad .

Documentation

- The display, the input procedures and the feedback of the reader device as well as the used test tool are to be documented.

C.3 Test Report

The test report must contain at least the following information:

- vendor and type designation of the reader device

- firmware version of the reader device
- driver version of the reader device
- Operating Systems used, version numbers of the installed patches (service packs, kernel versions, PCSC daemon)
- name and version number of the used eID-Client(s)
- test card used or simulator
- service portal used
- results of the described tests
- Any deviations from the described test instructions must be described in detailed and justified. The evaluation facility should conclude the test with an overall assessment of the functionality of the tested reader device.

D Support for PACE and EAC

If a card reader implements one of the modules A.4, A.5 or A.7, in order to support PACE and EAC according to [TR-03110] and [TR-03117]. The following commands have to be supported to the extent mandated by the implemented modules:

- Support for PACE channel:
  - GetReaderPACECapabilities
  - EstablishPACEChannel
  - DestroyPACEChannel
- Support for PIN Management inside a pre-established secure channel:
  - VerifyPIN
  - ModifyPIN

A mapping of these commands to PC/SC and CCID is given in sections D.2 and D.3, respectively.

D.1 Commands

D.1.1 GetReaderPACECapabilities

This command is used to query the PACE features supported by the card reader. This command takes no input and returns the following capabilities as supported:

- **PACE:** The reader supports PACE to establish a password authenticated secure channel between card reader and card, including the necessary user interaction (input of password).
- **eID**: The reader supports the eID function (Role Authentication Terminal) and, if the card reader has a display, shows eID data from the Terminal Certificate
- **eSign**: The reader supports QES with contactless cards according to [TR-03117] (Role Signature Terminal).
- **Destroy**: The reader supports explicit destruction of the PACE channel via DestroyPACEChannel. If not present, only implicit destruction, e.g. by a Secure Messaging error, is supported.

D.1.2 EstablishPACEChannel

The function EstablishPACEChannel is used to establish a password authenticated secure channel via the PACE protocol including the necessary user interaction.

The Input for this command comprises the following elements:

- Password-ID as defined in [TR-03110], i.e. one of the numerical values CAN → 2; PIN → 3; PUK → 4 – always present.
- Transmitted Password, may contain a password transmitted by the host – optional, must only be used for CAN. All other passwords must be rejected by the reader.
- Certificate Holder Authorization Template (CHAT), contains the CHAT (role identifier and access rights) which shall be transmitted to the card as part of PACE – must be present if authentication as Authentication Terminal (Capability eID) or Signature Terminal (eSign) is required. In the latter case the presence of the CHAT with role Signature Terminal signals the card reader to perform step 8 in the process description below.
- CertificateDescription, contains the Certificate Description as contained in the Terminal Certificate (see step 7 in the description below) – must be present if authentication as Authentication Terminal (Capability eID) is required.
- HashOID, contains the Object Identifier used for the hash computation of CertificateDescription (see step 4 in the description below), must be identical to the OID contained in the terminal certificate – optional, if not present the card reader shall assume SHA-256 as hash function.

The Output for this command comprises the following elements:

- The contents of EF.CardAccess as read from the card.
- Status words as returned by MSE:Set AT to convey the status of the password, e.g. if the password is blocked/suspended etc. (see [TR-03110]).
- The trust points (CAR_{cur} and CAR_{prev}) returned by the card in the final step of PACE, see [TR-03110] – present if authentication as Authentication Terminal (Capability eID) is required.
- The ephemeral public key of the terminal (ID_{PICC}), see [TR-03110] – present if authentication as Authentication Terminal (Capability eID) is required.
- Error Code as detailed below:

Code	***Description***
0x00000000	No Error
Error in input data	
0xD0000001	Inconsistent lengths in input
0xD0000002	Unexpected data in input
0xD0000003	Unexpected combination of data in input
Errors during protocol execution	
0xE0000001	Syntax error in TLV response
0xE0000002	Unexpected or missing object in TLV response
0xE0000003	Unknown Password-ID
0xE0000006	Wrong Authentication Token
0xE0000007	Certificate chain for terminal authentication cannot be built
0xE0000008	Unexpected data structure in response to chip authentication

0xE0000009	Passive authentication failed
0xE000000A	Incorrect token for chip authentication
Response APDU of the card reports error (status code SW1SW2)	
0xF000SW1SW2	Select EF.CardAccess
0xF001SW1SW2	Read Binary EF.CardAccess
0xF002SW1SW2	MSE: Set AT für PACE
0xF003SW1SW2 – 0xF006SW1SW2	General Authenticate Step 1-4
APDU created by PCD for terminal/chip authentication reports error (status code SW1SW2)	
0xF800SW1SW2	MSE: Set DST (first certificate)
0xF801SW1SW2	PSO: Verify Certificate (first certificate)
0xF802SW1SW2	MSE: Set DST (second certificate)
0xF803SW1SW2	PSO: Verify Certificate (second certificate)
0xF804SW1SW2	MSE: Set DST (third certificate)
0xF805SW1SW2	PSO: Verify Certificate (third certificate)
0xF806SW1SW2	MSE: Set AT for terminal authentication
0xF807SW1SW2	Get Challenge
0xF808SW1SW2	External Authenticate
0xF809SW1SW2	Select EF.CardSecurity
0xF80ASW1SW2	Read Binary EF.CardSecurity
0xF80BSW1SW2	MSE: Set AT for chip authentication
0xF80CSW1SW2	General Authenticate
Others	
0xF0100001	Communication abort (e.g. card removed during protocol)
0xF0100002	No card
0xF0200001	Abort
0xF0200002	Timeout

In the following the execution of the function EstablishPACEChannel is described:

1. The host computer invokes EstablishPACEChannel.
2. The card reader reads EF.CardAccess from the card and extracts the parameters necessary for PACE.
3. The card reader extracts from InputData
   - the Password-ID (PIN, CAN, PUK)
   - and – if available – the CHAT (Certificate Holder Authorization Template).
4. If the Role from the CHAT denotes an Authentication Terminal and a display is available: The card reader extracts the certificate description from InputData, retrieves and displays the certificate holder. If no certificate description has been provided, or the certificate holder cannot be displayed using the character set available in the card reader, the certificate holder is displayed as ‚Unknown'. Then, the access rights contained in CHAT will be displayed. The user can inspect them individually in the reader, but no further restrictions can be made. The reader computes the hash of the certificate description and stores it.

5. The card reader prompts for entering a password (if not included in the InputData) and derives K_π from it. If PIN or PUK are used as a password, the password must be entered at the PIN pad.
6. The card reader executes PACE using MSE:Set AT/General Authenticate according to [TR-03110] and computes the key material for the Secure Messaging between the card reader and the chip. The card reader clears all information from the memory which would allow conclusions on the PIN as soon as possible.
7. If a certificate description is included in InputData and a display is available: The commands, for which the card reader performs Secure Messaging, are monitored for "PSO:Verify Certificate" with Terminal Certificate. From the Terminal Certificate the Extension for the Certificate Description is extracted and the hash value from the Extension is compared to the value stored in step 4. If these two values are not identical, the command is blocked and status words SW1SW2 = 69 85 are returned.
8. If the Role from the CHAT denotes a Signature Terminal: After the establishment of the PACE channel the card reader performs Terminal Authentication and Chip Authentication. After a successful Chip Authentication, Secure Messaging with PACE keys is terminated and replaced by Secure Messaging using the newly negotiated keys.

D.1.3 DestroyPACEChannel

This command is used to close an established PACE channel. The session keys of the channel are deleted. This command has no Input and no Output.

D.1.4 VerifyPIN / ModifyPIN

These command are used to verify/modify a PIN inside a pre-established secure channel. Exact input and output are defined by the mappings in D.2 and D.3.

D.2 Mapping on PC/SC

In the case of PC/SC, the command from section D.1 are mapped to FEATURE_EXECUTE_PACE as defined in [PC/SC], part 10 amendment 1, and FEATURE_VERIFY_PIN_DIRECT / FEATURE_MODIFY_PIN_DIRECT as defined in [PC/SC], part 10.

The commands are mapped as follows:

- GetReaderPACECapabilities → FEATURE_EXECUTE_PACE/GetReaderPACECapabilities, the numerical values representing the Capabilities are given in [PC/SC], part 10 amendment 1.
- EstablishPACEChannel → FEATURE_EXECUTE_PACE/EstablishPACEChannel

  The InputData of EstablishPACEChannel as defined in [PC/SC], part 10 amendment 1, are extended by the following fields for support of the eID-function, for the conditions on the presence of these fields see the generic description in section D.1.2.

Number	*Type*	*Name*	*Description*
6	USHORT	length_CertificateDescription	Length of CertificateDescription
7	BYTE[]	CertificateDescription	Complete certificate description allowing the card reader to perform hash computation
8	USHORT	length_hashOID	Length of HashOID
9	BYTE[]	hashOID	Object Identifier of the Hash function used for the hash computation of CertificateDescription
Data types are used according to [PC/SC] part 9: USHORT → unsigned 16 bit, BYTE[] → array of unsigned 8 bit.			

- DestroyPACEChannel → FEATURE_EXECUTE_PACE/DestroyPACEChannel[6]
- VerifyPIN → FEATURE_VERIFY_PIN_DIRECT
- ModifyPIN → FEATURE_MODIFY_PIN_DIRECT

D.3 Mapping on CCID

For this mapping, the commands from D.1 are encapsulated in Pseudo-APDUs with the following structure:

	Command APDU					**Response APDU**	
	CLA	**INS**	**P1**	**P2**	**Command Data**	**Error Code**	**Response Data**
GetReaderPACE Capabilities	0xFF	0x9A	0x04	0x01	–	0x9000 – command successful other – execution error	`PACECapabilities`
EstablishPACE Channel				0x02	`EstablishPACEChannelInput`		`EstablishPACEChannelOutput`
DestroyPACEChannel				0x03	–		–
VerifyPIN / ModifyPIN				0x10	Coding of input as PC_to_RDR_Secure and output as RDR_to_PC_DataBlock as defined in [CCID].[7]		

The Command Data and Response Data are encoded as DER encoded ASN.1 structures (cf. [DER]) defined as follows:

```
PACECapabilities ::= SEQUENCE {
      capabilityPACE              [1] BOOLEAN
      capabilityEID               [2] BOOLEAN
      capabilityESign             [3] BOOLEAN
      capabilityDestroy           [4] BOOLEAN
}
EstablishPACEChannelInput ::= SEQUENCE {
      passwordID                  [1] INTEGER
      transmittedPassword         [2] NumericString OPTIONAL
```

6 This function may not be supported by card readers implemented according to version 1.2 or earlier of this TR. The support for this function is explicitly signalled as Capability, see [PC/SC], part 10 amendment 1.

7 The coding given here is an alternative to the commands in [CCID], which are not supported by all CCID stacks. A client application should preferably use the commands in [CCID], if available.

```
      cHAT                        [3] OCTET STRING OPTIONAL
            -- as defined in [TR-03110], including tag 0x7F4C
      certificateDescription      [4] CertificateDescription OPTIONAL
      hashOID                     [5] OBJECT IDENTIFIER OPTIONAL
}
EstablishPACEChannelOutput ::= SEQUENCE {
      errorCode                   [1] OCTET STRING (SIZE(4))
      statusMSESetAT              [2] OCTET STRING (SIZE(2))
      efCardAccess                [3] SecurityInfos
      idPICC                      [4] OCTET STRING OPTIONAL
            -- encoded as ephemeral public key (see [TR-03110])
      curCAR                      [5] OCTET STRING OPTIONAL
      prevCAR                     [6] OCTET STRING OPTIONAL
            -- *CAR encoded as Character Strings (see [TR-03110])
}
```

The types `CertificateDescription` and `SecurityInfos` are defined in [TR-03110].

E IT Security Evaluation

The fulfillment of IT-security requirements by a smart card reader has to be proved by an IT-security evaluation and certification according to the Common Criteria (Common Criteria for Information Technology Security Evaluation, Version 3.1). To a smart card reader without QES support, the evaluation level EAL3 augrmented with AVA_VAN.3 (and dependencies) has to be applied, to a card reader with QES support EAL3 augmented with AVA_VAN.5 (and dependencies).

It is recommended to base the certification on the Standard Reader Protection Profile [PP-0083].

The IT-security evaluation must be carried out by an evaluation facility recognised by the BSI according to DIN ISO/IEC 17025. The subsequent IT-security certification is granted by the BSI.

The “Security Target” (ST) serves as the central basis for an IT-security evaluation. The ST is created by the manufacturer of the smart card reader and must, depending on the type of reader, cover the following minimum requirements/functions:

- secure handling of the PINs entered, especially deletion of the PIN after use (module A.4).
- implementation PACE (e.g. key generation) (module A.4)
- compliance to filter rules (module A.4)
- if available: indication of the secure mode (module A.4)
- authentic display, especially correct display of the certificate authority and the access certificates when using the eID function (module A.5)
- protection against manipulation (modules A.4, A.5)
- securing and verifying the integrity of the firmware (module A.8)

If the smart card reader supports various applications or various security modes, a clear division of these applications and safe separation of the security modes is also part of the Security Target.

If the smart card reader supports the qualified signature, the Security Target must take into account the security requirements of the signature law. Finally, when supporting QES with the identity card the special test requirements form B.7 have to be covered.

Bibliography

[CP-eSign] BSI: Certificate Policy für die eSign-Anwendung des ePA

[PP-0083] BSI: Common Criteria Protection Profile BSI-CC-PP-0083, Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control

[PP-IS] BSI: Common Criteria Protection Profile for Inspection Systems, BSI-CC-PP-0064

[TR-03105] BSI: Technische Richtlinie TR-03105, Conformity Tests for Official Electronic ID Documents

[TR-03110] BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents

[TR-03116] BSI: Technische Richtlinie TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung

[TR-03117] BSI: Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit

[TR-03127] BSI: Technische Richtlinie TR-03127: Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel

[CEN 1332] CEN: prEN 1332-5 - Identification card systems – Man machine interface – Part 5: Raised tactile symbols for differentiation of application on ID-1 cards

[PP-SSCD] CEN: prEN 14169-1 -- Protection Profile for Secure signature creation device -- Part 2: Device with key generation, BSI-CC-PP-0059

[EMC] EMV: Integrated circuit card, Specification for Payment systems, Application independent ICC to terminal interface requirements

[EMV] EMV: Integrated circuit card, Specification for Payment systems, Application independent ICC to terminal interface requirements

[ICAO 9303] ICAO: Doc 9303, Machine Readable Travel Documents, Part 3

[ISO 14443] ISO/IEC: ISO 14443 - Identification cards – Contactless integrated circuit(s) cards – Proximity cards

[ISO 7810] ISO/IEC: ISO 7810 - Identification cards - Physical characteristics

[ISO 7816] ISO/IEC: ISO 7816 - Identification cards – Integrated circuit cards

[ISO 10373] ISO/IEC: ISO/IEC 10373 -- Identification cards -- Test methods

[DER] ITU-T: Information Technology – ASN.1 encoding rules: Specification of Basic Encoding Rules(BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

[PC/SC] PC/SC Workgroup: PC/SC Workgroup Specifications 1.0/2.0

[MKT] TeleTrust: Multifunktionale KartenTerminals MKT-Spezifikation – MKT-Version 1.0

[CCID] USB Implementers Forum: Universal Serial Bus -- Device Class: Smart Card CCID -- Specification for Integrated Circuit(s) Cards Interface Devices